

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

## UNITED STATES DISTRICT COURT

for the  
District of New MexicoIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)3650 NM Highway 528 NE, Rio Rancho, NM 87144  
units #50 and #7

Case No. MR 21-973

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_ New Mexico \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1030(a)(4)	Fraud and Related Activity in Connection with Computers
18 U.S.C. § 1343	Fraud by wire, radio or television

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Special Agent Andrea Coffey

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone \_\_\_\_\_ (specify reliable electronic means).

Date: 07/16/2021

City and state: Albuquerque, New Mexico

  
Judge's signature

Jerry H. Ritter

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:  
3650 NM Highway 528 NE, Rio Rancho, NM  
87144 units #50 and #7

Case No.

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR AN SEARCH WARRANT**

I, Andrea Coffey, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of criminal Procedure for a warrant to search the premises known as 3650 NM Highway 528 NE, Rio Rancho, NM 87144 units #50 and #7, herein after the PREMISES, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since March, 2020. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime. I have gained experience through training and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I worked as a police officer and detective for six years investigating crimes related to fraud, property crimes and violent crimes. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 1030(a)(4) and 18 U.S.C. § 1343, and I am authorized by the Attorney General to request a search warrant.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit is personally known to me based on my training and

experience, was gathered or revealed to me personally during the course of this investigation, or was gathered or revealed to other sworn law enforcement officers during the course of this investigation and subsequently communicated to me.

4. Based on the information set forth herein, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(4) (Fraud and Related Activity in Connection with Computers), and 18 U.S.C. § 1343 (Fraud by wire, radio or television) were committed, and that evidence of these violations may be found within THE PREMISES.

#### PROBABLE CAUSE

##### ***Background & Terms***

##### *Internet Service Providers*

5. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses with access to the Internet through access accounts. Subscribers obtain an account by registering with ISPs. During the registration process, ISPs ask subscribers to provide basic personal information. Additionally, ISPs are likely to maintain records and information concerning subscribers and their use of the ISP’s services, such as account use and access information and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

##### *IP Addresses*

6. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses are provided by ISPs and are used to identify a computer on a network. IP addresses can be “dynamic,” meaning that the ISP assigns a different

unique number to a computer every time it accesses the Internet. IP addresses might also be “static” if an ISP assigns a user’s computer a particular IP address, which is used each time the computer accesses the Internet. In my training and experience, ISPs commonly maintain records of which subscriber used an IP address, and the period of time for which that subscriber used that IP address. As such, the identification of an IP address that used an internet service, such as Google Translate, at a given time can lead to the identification of the individual subscriber.

***Background on 18 U.S.C. § 1343***

7. 18 U.S.C. § 1343 criminalizes conduct by which someone “[...] devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce [...]” Therefore, relevant to the investigation described below, I believe that when someone obtains money fraudulently by wire, they have violated 18 U.S.C. § 1343.

***Background on 18 U.S.C. § 1030(a)(4)***

8. 18 U.S.C. § 1030(a)(4) criminalizes conduct by which someone “[...] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [...]” 18 U.S.C. § 1030(e)(2) defines a protected computer to include a computer “which is used in or affecting interstate or foreign commerce or communication.” Therefore, relevant to the investigation described below, I believe that when someone accesses a protected computer without authorization, they have violated 18 U.S.C. § 1030(a)(4).

### *House of Sanjevani*

9. House of Sanjevani, herein after THE VICTIM, is a holistic wellness center with a location in Albuquerque, New Mexico. THE VICTIM also provides wellness products such as vitamins, minerals and oils via their online store. THE VICTIM sells to clients nationally and internationally, thus having an impact on interstate commerce. THE VICTIM is owned and operated by SP and MS.

### *The Investigation*

10. On or about July 23, 2020, The FBI learned of a potential wire fraud case, referred to the Albuquerque Field Office by the Albuquerque Police Department (APD). SP reported to APD in March 2020 that he had become aware of issues with his profits after noticing a dramatic decrease in sales on a weekend that specials were available in THE VICTIM online store. THE VICTIM website and online store are operated by the ecommerce platform Shopify. When purchases are made, the payments are processed through Authorize.net. Authorize.net is separate from Shopify and is the payment processor that SP has chosen to use for his online sales. After looking into the issue, SP noticed that the online store payment processor had been changed from the initial processor, Authorize.net, to a processor not contracted by SP, Stripe. After further investigation, SP determined that this had been occurring since on or about May 3, 2019.

11. SP discovered that between May 2019 and March 2020, approximately \$112,000 was rerouted from the payment processor of Authorize.net via the Stripe payment processor, and potentially via other payment processors currently unknown, into an unknown bank account. SP contacted Shopify and obtained the IP address that was utilized to make the unauthorized changes in March 2020: 184.155.117.139. I then served a subpoena to Shopify requesting all IP

addresses used to access THE VICTIM'S Shopify account and learned that IP address 184.155.117.139 had been used to access THE VICTIM'S Shopify account from December 2019 through March 2020. Also shown on the return from Shopify was an email address connected to the account, alex@sanjevani.net. SP advised that Alexander Sutton used to be employed for THE VICTIM as the 'IT guy' and that Sutton is familiar with how business is conducted and how payments are processed for THE VICTIM.

12. FBI Agents were provided the above information and further analysis of this IP address through open source research revealed that it resolved to Rio Rancho, New Mexico and was owned by Cable One, Inc. Court process on Cable One, Inc. returned that the IP address 184.155.117.139 was assigned to Alex Sutton from August 30, 2019 through August 6, 2020. Cable One, Inc provided account information for Alex Sutton. The account for Alex Sutton has a contact phone number, 505-231-2461. And a customer address of 6426 Oersted Road NE, Rio Rancho, NM 87144. The assignment of the IP address in question corresponds with a portion of the dates that the unauthorized transactions were taking place, most notably the ones taking place when SP discovered the discrepancy in the payment processors.

13. Further investigation revealed a bank account held at The Bancorp belonging to Alexander Sutton. The Bancorp is an online banking institution that is based in Wilmington, DE and provides deposit and loan accounts as well as prepaid access cards. Court process served on The Bancorp returned information for Alexander Sutton's account, number 42322230132049995. One of the account identifiers on the account is a phone number, 505-231-2461 as well as a birthday of August 26, 1984. The account also shows a customer address of 6426 Oersted Road NE, Rio Rancho, NM 87144. Statements show that there are over 40 direct deposit transactions into the account beginning on May 3, 2019 of varying amounts with deposit

dates inconsistent with any payroll or other scheduled payments. Additionally, details of each direct deposit were provided, showing that the source of these deposits include the payment processor, Stripe, among other sources of deposits. The Bancorp offers access to client accounts from the main website as well as through their phone application, allowing access from desktop computers, laptop computers, tablets and cellular phones.

14. Based on the above information, I believe that Alexander Sutton, using the IP address 184.155.117.139, accessed THE VICTIM'S computer without authorization, and had funds rerouted from THE VICTIM'S payment processor and account to an account of his own, and in doing so violated 18 U.S.C. § 1030(a)(4) as well as 18 U.S.C. § 1343.

*Confirming Alexander Sutton's Identity*

15. On or about July 29, 2020, Special Agent (SA) Jacob vanBrandwijk requested the FBI Albuquerque Operations Center query New Mexico Driver's License databases for records related to Alexander Sutton, as well as a query of the National Crime Information Center (NCIC) databases for the same person. Additionally, on or about August 11, 2020, SA vanBrandwijk obtained a record from the Accurant database for Alexander Sutton. Alexander Sutton's driver's license records as well as the record for Alexander Sutton, who has a birthday of August 8, 1984, show an address of 6426 Oersted Road NE, Rio Rancho, NM 87144.

*Locating Sutton*

16. In the information obtained via NCIC on Sutton, it was learned that Sutton is under supervised probation. Sutton is currently under the supervision of Officer Steven Muller. Officer Muller advised the Sutton had been arrested on a probation violation and was currently undergoing treatment in Los Lunas at the Men's Recovery Center located in Los Lunas, New Mexico. Sutton is set to be released from the Recovery Center on July 20, 2021.



17. In July 2021, SA Andrea Coffey contacted Officer Muller and obtained the address that Sutton will be living upon release: 53 Pinon Ridge Road, Pecos, NM 87535. Officer Muller advised that Sutton will be transferred to the Santa Fe division of probation and parole under the supervision of Officer Sariah Gonzales once he is released, as Sutton's new address is covered by the Santa Fe division of probation and parole. During his time at the Recovery Center, Sutton has not been allowed to possess or access any computers or cellular phones. In July 2021, Officer Muller learned from Sutton that once he is released, Sutton will have access to two cellular phones and one computer.

18. On or about July 1, 2021 SA Coffey contacted Officer Gonzales. Officer Gonzales, per policies in place at New Mexico Corrections Department - Probation and Parole, is required to check the address that Sutton has provided to ensure that it is suitable for Sutton to reside at to be within regulations of his felon status. During the check of the residence on July 14, 2021, Office Gonzales learned that before Sutton went into recovery, he and his girlfriend rented storage units for his belongings. This storage unit is located in Rio Rancho. During the residence check, there were no belongings of Sutton's in the home.

19. In an interview with Anwar Alaghberry, manager of the Stagecoach Stop RV Park located at 3650 NM Highway 528 NE, Rio Rancho, NM 87144, it was learned that Sutton has rented units #50 and #7. On July 15, 2021, I confirmed with Brad Varney, an employee at Stagecoach Stop RV Park, that Sutton still currently rents units #50 and #7.

20. Based on the information above, I believe that Sutton presently has his belongings stored at 3650 NM Highway 528 NE, Rio Rancho, NM 87144 in units #50 and #7, THE PREMISES.



*Tools used in Criminal Activity in THE PREMISES*

21. As previously mentioned, Sutton is able to access his online banking account with The Bancorp on electronic devices, including: desktop computers, laptop computers, tablets and cellular phones. Additionally, Shopify and Stipe also offer a mobile application for users to manage their accounts from mobile devices. The unauthorized activity on Shopify, the ecommerce platform used by the VICTIM, is also accessible on numerous types of electronic devices allowing the changing of payment processors for the platform. Additionally, Sutton told Officer Muller that he would have access to two phones and a computer once released. It is reasonable to believe that these are the same phones and computers that Sutton had access to prior to his arrest and assignment into treatment at the Recovery Center. I therefore believe that devices used to carry out the above described crimes may be found in THE PREMISES.

*Evidence of a Crime in THE PREMISES*

22. I know that computers, cellular devices, and other electronic devices record and store a great wealth of information regarding when and how they are used, and who is using them. This information is further described in the section below entitled "COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS." Because of the ubiquity of such devices as mechanisms of communication or as tools to access online market places, I believe that it is likely that any such devices which likely to have been used by Sutton may contain evidence of the execution of the unauthorized access to a protected computer as well as wire fraud related to the unauthorized access of the protected computer. I further know, based on my training and experience and my experience with the incident investigation, that network devices may maintain logs of which computers were connected to such devices (and thus ultimately connected to the internet), such as the devices used to carry out these crimes.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

23. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.  
  
Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or

exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to

destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to perform a denial of service attack, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime.

The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

26. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large



volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

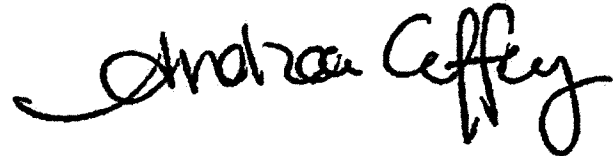
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

28. Based on the aforementioned information and investigation, I submit that probable cause exists to search THE PREMISES, as more particularly described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,



---

Andrea Coffey  
Special Agent  
Federal Bureau of Investigation

Submitted electronically and sworn telephonically on July 16, 2021



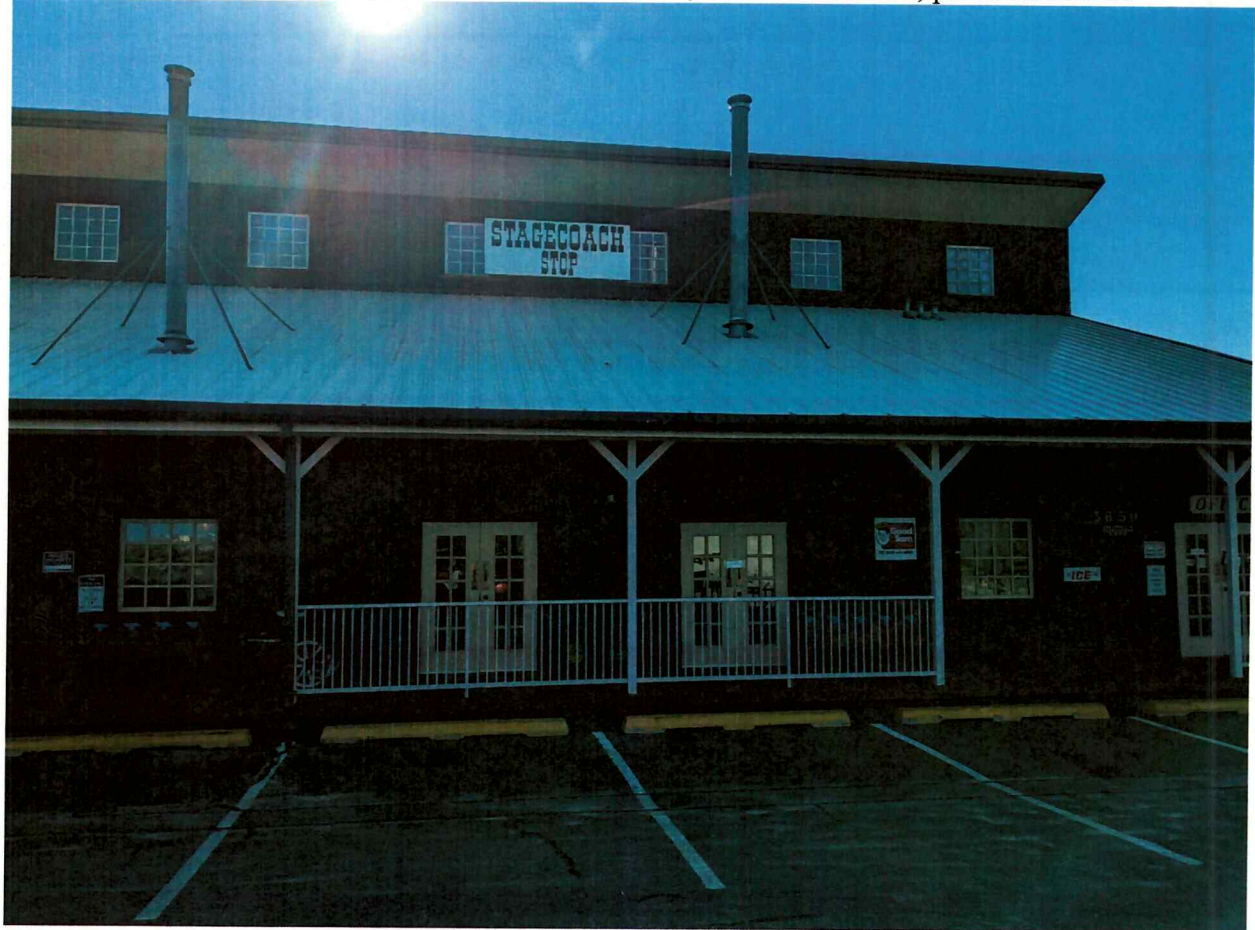
---

Honorable Jerry H. Ritter  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

***Property to be searched***

3650 NM Highway 528 NE, Rio Rancho, NM 87144, units #50 and #7, pictured below:





Unit #50





Unit #7





ATTACHMENT B

*Property to be seized*

1. Records relating to financial accounts serviced by The Bancorp, or financial accounts in the names of Alexander Sutton and/or The House of Sanjevani including:
  - a. Records created by financial institutions, such as signature cards, bank statements, or other documents;
  - b. written documents, including handwritten and typed documents related to online access of financial accounts, such as password lists, website addresses, account numbers and user names; and
  - c. records of transactions, such as deposit slips, cash withdrawal receipts, wire or money services transfer records.
2. Records relating to mobile phone service and internet service.
3. Drivers licenses, mail, or other documents bearing Alexander Sutton's name or personal identifiers.
4. Any other records and information relating to violations of 18 U.S.C. §§ 1030 and 1343, those violations involving Alexander Sutton, or others yet unknown.
5. Any and all electronic devices which may have been used as a means to commit the violations described above, and/or may contain any electronically stored information pertaining to the violations described above, hereafter THE DEVICES, including desktop computers, laptops, tables, cellular telephone devices, and electronic storage devices.
6. Passwords, encryption keys, and other access devices that may be necessary to access THE DEVICES.
7. Documentation and manuals that may be necessary to access THE DEVICES or to conduct a forensic examination of THE DEVICES.
8. All records or information, contained in or on THE DEVICES, in whatever form they may be found, relating to violations 18 U.S.C. §§ 1030 and 1343, those violations involving Alexander Sutton, or others yet unknown, including:
  - a. financial records, such as those listed in item 1 of this attachment;
  - b. mobile phone records, such as those listed in item 2 of this attachment;
  - c. records relating to Alexander Sutton's personal information, such as those listed in item 3 of this attachment;



- d. all records, e-mails, text messages, or other communications between subjects known and unknown to us related to schemes in violation of 18 U.S.C. §§ 1030 and 1343;
- e. evidence of who used, owned, or controlled THE DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- f. evidence of software that would allow others to control THE DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- g. evidence of the lack of such malicious software;
- h. evidence indicating how and when THE DEVICES were accessed or used to determine the chronological context of device access, use, and events relating to crime under investigation and to the computer user;
- i. evidence indicating THE DEVICES user’s state of mind as it relates to the crime under investigation;
- j. evidence of the attachment to THE DEVICES of other storage devices or similar containers for electronic evidence;